AMENDMENTS TO THE CLAIMS

Please amend claims 6, 8, 11, 16-17, and 20; cancel claims 1-5, 10, 12-15, and 22-68; and add new claims 69-102. All pending claims are reproduced below.

1-5. (Cancelled)

6. (Currently Amended) ~~A method as recited in claim 1,~~ A computer-implemented method of implementing security for Simple Object Access Protocol (SOAP) messages which can be exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one decryption rule[[,]]; and

performing at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of the at least one operation comprises:

determining whether the SOAP message is encrypted, and

decrypting the SOAP message based on one or more decryption keys which are associated with the at least one decryption rule.

7. (Original) A method as recited in claim 6, wherein the one or more decryption keys are managed by an organization or define an organizational rule.

8. (Currently Amended) ~~A method as recited in claim 1,~~ A computer-implemented method of implementing security for Simple Object Access Protocol (SOAP) messages which can be exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for

exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one encryption rule[[,]]; and

performing at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of at least one operation comprises:

encrypting the SOAP message based on one or more encryption keys which are associated with the at least one encryption rule.

9. (Original) A method as recited in claim 8, wherein the one or more encryption keys are associated with an individual.

10. (Cancelled)

11. (Currently Amended) A method as recited in claim 6, wherein the method further comprises:

determining whether the SOAP message has been ~~encrypted~~ decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been ~~encrypted~~ decrypted successfully.

12-15. (Cancelled)

16. (Currently Amended) A computer-implemented method of implementing security for Simple Object Access Protocol (SOAP) messages exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one decryption rule is associated with the SOAP message;

attempting to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determining whether at least one encryption rule is associated with the SOAP message;

encrypting the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message;

determining whether at least one signature verification rule is associated with the SOAP message;

verifying at least one signature associated with the SOAP message per requirements specified by the at least one signature verification rule when the determining determines that at least one signature verification rule is associated with the SOAP message;

determining whether at least one signing rule is associated with the SOAP message; and

signing the SOAP message using one or more keys associated with the at least one signing rule.

17. (Currently Amended) A computer readable medium having computer program instructions stored therein for performing ~~the method of claim 16.~~ a method of implementing security for Simple Object Access Protocol (SOAP) messages exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one decryption rule is associated with the SOAP message;

attempting to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determining whether at least one encryption rule is associated with the SOAP message;

encrypting the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message;

determining whether at least one signature verification rule is associated with the SOAP message;

verifying at least one signature associated with the SOAP message per requirements specified by the at least one signature verification rule when the determining

determines that at least one signature verification rule is associated with the SOAP message;

determining whether at least one signing rule is associated with the SOAP message; and

signing the SOAP message using one or more keys associated with the at least one signing rule.

18. (Original) A method as recited in claim 16, wherein the method further comprises:

determining a message type for the SOAP message, and

looking up rules which are associated with the message type.

19. (Original) A method as recited in claim 16, wherein at least one portion of the SOAP message is XML.

20. (Currently Amended) A method as recited in claim 16, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determining whether the SOAP message has been ~~encrypted~~ decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been ~~encrypted~~ decrypted successfully.

21. (Original) A method as recited in claim 16, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that the at least one signature has not been successfully verified.

22-68. (Cancelled)

69. (New) The computer readable medium of claim 17, wherein the method further comprises:

determining a message type for the SOAP message, and

looking up rules which are associated with the message type.

70. (New) The computer readable medium of claim 17, wherein at least one portion of the SOAP message is XML.

71. (New) The computer readable medium of claim 17, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determining whether the SOAP message has been decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

72. (New) The computer readable medium of claim 17, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that the at least one signature has not been successfully verified.

73. (New) A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a Simple Object Access Protocol (SOAP) message;

determine whether at least one decryption rule is associated with the SOAP message;

attempt to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determine whether at least one encryption rule is associated with the SOAP message;

encrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message;

determine whether at least one signature verification rule is associated with the SOAP message;

verify at least one signature associated with the SOAP message per requirements specified by the at least one signature verification rule when the determining determines that at least one signature verification rule is associated with the SOAP message;

determine whether at least one signing rule is associated with the SOAP message; and

sign the SOAP message using one or more keys associated with the at least one signing rule.

74. (New) The traffic manager of claim 73, wherein the central processing unit can further operate to:

determine a message type for the SOAP message, and

look up rules which are associated with the message type.

75. (New) The traffic manager of claim 73, wherein at least one portion of the SOAP message is XML.

76. (New) The traffic manager of claim 73, wherein the central processing unit can further operate to:

determine whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determine whether the SOAP message has been decrypted successfully; and

take appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

77. (New) The traffic manager of claim 73, wherein the central processing unit can further operate to:

determine whether the at least one signature associated with the SOAP message has successfully been verified; and

take appropriate action when the determining determines that the at least one signature has not been successfully verified.

78. (New) A computer readable medium having computer program instructions stored therein for performing a method of implementing security for Simple Object Access Protocol (SOAP) messages which can be exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one decryption rule; and

performing at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of the at least one operation comprises:

determining whether the SOAP message is encrypted, and

decrypting the SOAP message based on one or more decryption keys which are associated with the at least one decryption rule.

79. (New) The computer readable medium of claim 78, wherein the one or more decryption keys are managed by an organization or define an organizational rule.

80. (New) The computer readable medium of claim 78, wherein the method further comprises:

determining whether the SOAP message has been decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

81. (New) A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a Simple Object Access Protocol (SOAP) message;

determine whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one decryption rule; and

perform at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of the at least one operation comprises:

determining whether the SOAP message is encrypted, and

decrypting the SOAP message based on one or more decryption keys which are associated with the at least one decryption rule.

82. (New) The traffic manager of claim 81, wherein the one or more decryption keys are managed by an organization or define an organizational rule.

83. (New) The traffic manager of claim 81, wherein the central processing unit can further operate to:

determine whether the SOAP message has been decrypted successfully; and

take appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

84. (New) A computer readable medium having computer program instructions stored therein for performing a method of implementing security for Simple Object Access Protocol (SOAP) messages which can be exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one encryption rule; and

performing at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of at least one operation comprises:

encrypting the SOAP message based on one or more encryption keys which are associated with the at least one encryption rule.

85. (New) The computer readable medium of claim 84, wherein the one or more encryption keys are associated with an individual.

86. (New) A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a Simple Object Access Protocol (SOAP) message;

determine whether at least one security rule has been defined for the SOAP message, the at least one security rule being defined based on a security policy for exchanging SOAP messages between at least one client program and at least one server program, wherein the at least one security rule includes at least one encryption rule; and

perform at least one security related operation on the SOAP message based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message, wherein the performing of at least one operation comprises:

encrypting the SOAP message based on one or more encryption keys which are associated with the at least one encryption rule.

87. (New) The traffic manager of claim 86, wherein the one or more encryption keys are associated with an individual.

88. (New) A computer-implemented method of implementing security for Simple Object Access Protocol (SOAP) messages exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one decryption rule is associated with the SOAP message;

attempting to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determining whether at least one encryption rule is associated with the SOAP message; and

encrypting the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message.

89. (New) A method as recited in claim 88, wherein the method further comprises:

determining a message type for the SOAP message, and

looking up rules which are associated with the message type.

90. (New) A method as recited in claim 88, wherein at least one portion of the SOAP message is XML.

91. (New) A method as recited in claim 88, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determining whether the SOAP message has been decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

92. (New) A method as recited in claim 88, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that the at least one signature has not been successfully verified.

93. (New) A computer readable medium having computer program instructions stored therein for performing a method of implementing security for Simple Object Access Protocol (SOAP) messages exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one decryption rule is associated with the SOAP message;

attempting to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determining whether at least one encryption rule is associated with the SOAP message; and

encrypting the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message.

94. (New) The computer readable medium of claim 93, wherein the method further comprises:

determining a message type for the SOAP message, and

looking up rules which are associated with the message type.

95. (New) The computer readable medium of claim 93, wherein at least one portion of the SOAP message is XML.

96. (New) The computer readable medium of claim 93, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determining whether the SOAP message has been decrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

97. (New) The computer readable medium of claim 93, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that the at least one signature has not been successfully verified.

98. (New) A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a Simple Object Access Protocol (SOAP) message;

determine whether at least one decryption rule is associated with the SOAP message;

attempt to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determine whether at least one encryption rule is associated with the SOAP message; and

encrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message.

99. (New) The traffic manager of claim 98, wherein the central processing unit can further operate to:

determine a message type for the SOAP message, and

look up rules which are associated with the message type.

100. (New) The traffic manager of claim 98, wherein at least one portion of the SOAP message is XML.

101. (New) The traffic manager of claim 98, wherein the central processing unit can further operate to:

determine whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determine whether the SOAP message has been decrypted successfully; and

take appropriate action when the determining determines that the SOAP message has not been decrypted successfully.

102. (New) The traffic manager of claim 98, wherein the central processing unit can further operate to:

determine whether the at least one signature associated with the SOAP message has successfully been verified; and

take appropriate action when the determining determines that the at least one signature has not been successfully verified.